UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/718,024	11/20/2000	Jukka Alve	4925-80	9643

7590 08/06/2004

Michael C Stuart Esq
Cohen Pontani Lieberman & Pavane
551 Fifth Avenue
Suite 1210
New York, NY 10176

EXAMINER
KIM, JUNG W

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/718,024	**Applicant(s)** ALVE ET AL.	
	Examiner Jung W Kim	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on ____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-34 is/are pending in the application.

4a) Of the above claim(s) ____ is/are withdrawn from consideration.

5)□ Claim(s) ____ is/are allowed.

6)☒ Claim(s) 1-34 is/are rejected.

7)□ Claim(s) ____ is/are objected to.

8)□ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 16 March 2001 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. ____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 9/18/02,5/30/02.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: ____.

DETAILED ACTION

1. Claims 1-34 have been examined.

Specification

2. The disclosure is objected to because of the following informalities: on page 14, lines 9-11, the sentence is not grammatical. Appropriate correction is required.

Claim Objections

3. Claim 24 is objected to because of the following informalities: regarding claim 24, the claim refers to the method of claim 23; however claim 23 defines an apparatus. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 6 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claim 6 recites the limitation "the recorded data stream" in line 7. There is insufficient antecedent basis for this limitation in the claim.

7. Claims 10-12 and 22-30 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. The omitted structural cooperative relationships are: an IC tester with means to request access for and receive an internal key stored on a one-time programmable ROM, wherein a readout path connects the tester with the first and second irrevocable conditions and the one-time programmable ROM. These structural features are critical to define the interrelated association between the first irrevocable condition and the second irrevocable condition, and the restrictions placed the request for key access by the tester and the conditional passing of the internal key from ROM to the tester. Furthermore, the only embodiments disclosed by the applicant in the specification in regards to the limitations of these claims disclose an IC tester with means to request a key and receive a key from memory of the recording/playback apparatus. See applicant's specification, Figure 5 and pages 12-14.

8. Claims 10-12 and 22-20 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: disabling the path essential to functioning of the recording and playback device by the second irrevocable condition **when** the second irrevocable condition re-enables the readout path for at least a portion of the encryption key. This step is essential to define the interleaved

relationship between the step of requesting a stored key and the step of disabling the recording and playback features of the device.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

10. Claims 1, 2, 6, 7, 13, 14, 18, 19, 31 and 32 are rejected under 35 U.S.C. 102(e) as being anticipated by Maillard et al. U.S. Patent No. 6,714,650 (hereinafter Maillard).

11. As per claim 13, Maillard discloses an apparatus for recording and playing back digital data (see Maillard, Figure 3), comprising:

a. a data receiver for receiving packets of a digital data stream (see Maillard, Figure 3, Reference Nos. 13 and 40; col. 7, lines 30-43);

b. an encrypter for encrypting the packets according to an encryption key unique to the apparatus (see Maillard, Figure 3, Reference No. 6; col. 7, lines 53-65; col. 8, lines 9-16, especially line 12); and

c. a data store for storing the encrypted packets (see Maillard, Figure 3, Reference No. 43).

The aforementioned covers claim 13.

12. As per claim 14, Maillard discloses an apparatus as outlined above in the claim 13 rejection under 35 U.S.C. 102(e). In addition, the apparatus further comprises:

d. a decrypter for retrieving and decrypting the encrypted packets according to the encryption key unique to the apparatus (see Maillard, Figure 3, Reference No. 42; col. 7, lines 35-38; col. 8, lines 9-16); and

e. a data transmitter for passing the decrypted packets to a presentation device (see Maillard, Figure 3, Reference No. 44);

f. whereby a copy of the encrypted packets will not play back intelligibly using a different apparatus (see Maillard, col. 8, lines 9-16, especially line 12),

g. whereby the encrypted packets are protected against unauthorized distribution (see Maillard, Abstract; col. 1, line 1-col. 4, line 58; col. 8, lines 9-16; Figure 3, Reference No. 43).

The aforementioned covers claim 14.

13. As per claim 18, Maillard discloses an apparatus as outlined above in the claim 13 rejection under 35 U.S.C. 102(e). In addition, a packet comprises a first predetermined number of header bytes and a second predetermined number of payload bytes; the data store stores the header bytes unencrypted; and the data store stores the payload bytes encrypted, whereby operations performable on the data stream that require access to header bytes but not to payload bytes are performable on the recorded data stream. See Maillard, Figure 4; col. 8, lines 28-35. The aforementioned covers claim 18.

14. As per claim 19, Maillard discloses an apparatus as outlined above in the claim 18 rejection under 35 U.S.C. 102(e). In addition, the stored packets are retrieved from the data store, header bytes are not decrypted, and payload bytes are decrypted by the decrypter. See Maillard, Figure 4; col. 8, lines 47-57. The aforementioned covers claim 19.

15. As per claims 1, 2, 6 and 7, they are method claims corresponding to claims 13, 14, 18 and 19, and they do not teach or define above the information claimed in claims 13, 14, 18 and 19. Therefore, claims 1, 2, 6 and 7 are rejected as being anticipated by Maillard for the same reasons set forth in the rejections of claims 13, 14, 18 and 19.

16. As per claims 31 and 32, Maillard discloses an apparatus as outlined above in the claim 13 and 14 rejections under 35 U.S.C. 102(e). In addition, the apparatus is a set-top box. See Maillard, Figure 2. The aforementioned cover claims 31 and 32.

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

19. Claims 3, 4, 5, 15, 16, 17, 33 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maillard in view of Fielder et al. U.S. Patent No. 5,963,646 (hereinafter Fielder) and Reardon U.S. Patent No. 6,212,635 (hereinafter Reardon).

20. As per claims 15-17, Maillard discloses an apparatus as outlined above in the claim 13 rejection under 35 U.S.C. 102(e). Maillard teaches the use of a plurality of keys unique to the apparatus used to decrypt the audio and visual data but does not expressly disclose that an encryption key is formed according to a predetermined algorithm from a first portion and a second portion, wherein one of the portions are stored in permanent storage. See Maillard, col. 4, lines 13-18; col. 7, lines 53-61; col. 8, lines 6-16 and 50-52. Fielder teaches a secure encryption key generator system which combines multiple values to derive a deterministic encryption key wherein at least one of the values are stored in permanent storage. See Fielder, claim 12, col. 9, line 64 and col. 10, lines 2 and 3. It would be obvious to one of ordinary skill in the art at the time the invention was made for the encryption key used in Maillard to be formed according to a predetermined algorithm from a first portion and a second portion since this means enables a non-predictable but deterministic key to be generated. See Fielder, Abstract. Finally, Maillard does not disclose the seed values used to form the encryption key as values unique to the apparatus. However, seeds specific to a user/device are common implementations in the art to cryptographically bind an encryption key to a profile. For example, Reardon teaches incorporating seed values specific to a user and a computer configuration to uniquely associate the key to a user/device profile wherein the user seed value is received through a user interface and entered by a user, and the device seed value is acquired from the device itself. See Reardon, col. 10, lines 40-59. By applying the deterministic algorithm to the method of Maillard, the seed values represents values specific to the user/device profile, and the constant value represents

one of the plurality of encrypted control words associated with an audio/visual data stream and stored in memory, wherein the user is authorized to access, and wherein a certain one of the plurality of encrypted control words is selected to decrypt a certain portion of the audio/visual data stream. See Maillard, col. 7, lines 55-61. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the portions that form the encryption key to include values unique to the apparatus and/or the user, wherein the user by means of a user interface enters the value unique to the user and the device supplies the values unique to the device. Motivation for such a combination enables the encryption key to be formed sufficiently unique to the user/device profile. Ibid. The aforementioned cover claims 15-17.

21. As per claims 3-5, they are method claims corresponding to claims 15-17, and they do not teach or define above the information claimed in claims 15-17. Therefore, claims 3-5 are rejected as being obvious over Maillard in view of Fielder and Reardon for the same reasons set forth in the rejections of claims 15-17.

22. As per claims 33 and 34, they are apparatus claims corresponding to claims 15-17, and they do not teach or define above the information claimed in claims 15-17. Therefore, claims 33 and 34 are rejected as being obvious over Maillard in view of Fielder and Reardon for the same reasons set forth in the rejections of claims 15-17.

23. Claims 8 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maillard in view of Chaney U.S. Patent No. 5,852,290 (hereinafter Chaney).

24. As per claim 20, Maillard discloses an apparatus as outlined above in the claim 19 rejection under 35 U.S.C. 102(e). Maillard does not expressly disclose control logic to replace the header bytes when stored packets are retrieved from the data store then decrypted. However, header bytes of an audio/visual packet include information pertaining to the status of the packet. When the status of the packet changes, the header data must change to correspond with the changes to the packet in order for the header data to maintain relevancy. For example, Chaney teaches multiple flags within a header that specify the current status of a given packet. See Chaney col. 5, Table 2 and related text. Further, since the packets are decrypted, the contents of the stream would not include messages specific to decryption of the packets, and hence, the flags specified by Chaney would necessarily be flipped to 0. Ibid. It would be obvious to one of ordinary skill in the art at the time the invention was made for the header bytes to be replace by control logic when the stored packets are retrieved from the data store then decrypted so that the header data maintains the current status of the decrypted packets as known to one of ordinary skill in the art. The aforementioned covers claim 20.

25. As per claim 8, it is a method claim corresponding to claim 20, and it does not teach or define above the information claimed in claim 20. Therefore, claim 8 is

rejected as being obvious over Maillard in view of Chaney for the same reason set forth in the rejection of claim 20.

26. Claims 10-12 and 22-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maillard in view of Fielder and Reardon, and further in view of Habersetzer et al. U.S. Patent No. 5,627,478 (hereinafter Habersetzer) and Cromer et al. U.S. Patent No. 6,105,136 (hereinafter Cromer).

27. As per claim 25, Maillard discloses a recorder as outlined above in the claim 14 and 15 rejections under 35 U.S.C. 102(e) and 103(a). Maillard does not teach an arrangement wherein an encryption key retrieval is disabled/re-enabled by conditions. However, means for restricted reading of an encryption key based on a set of conditions is a conventional feature in the art for reasons that include, inter alia, user access privileges, request validity and memory integrity validation to check for evidence of tampering. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for an encryption key retrieval means to be disabled/re-enabled by relevant conditions to ensure that key usage is limited only to authorized circumstances as known to one of ordinary skill in the art.

28. Further, Maillard does not teach a disabling first condition and a re-enabling second condition for a read-out path of the encryption key. Habersetzer teaches a circuitry configuration in an apparatus to ensure proper selected entry into and out of a

mode. See Habersetzer, col. 1, lines 40-42; Figure 5, Reference No. 32. It would be obvious to one of ordinary skill in the art at the time the invention was made for the encryption key retrieval read-out path to be disabled by a first condition and re-enabled by a second condition to prevent inadvertent entry into and out of a mode. Ibid.

29. Further, Maillard does not teach disabling the recording and playback features based on a condition. However, means to disable the features of a device when improper usage is detected is a common implementation in the art of security. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art the time the invention was made to disable the recording and playback features based on a condition to disrupt improper usage of the device as known to one of ordinary skill in the art.

30. Further, Maillard does not teach the condition to disable the recording and playback features as the second condition. However, it is common in the art for multiple features to be enabled/disable together under circumstances that may compromise the nature of a device as expressed above. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for the second condition to disable the recording and playback features since sensitive stored information within a device and the proper functioning of the device are two features which need to be secured when tampering or improper usage is detected as known to one of ordinary skill in the art.

31. Finally, Maillard does not teach the two conditions as irrevocable. In the circumstances of tampering or improper use, a revocable condition enables a

perpetrator to continuously attempt to access or use a restricted device by resetting the condition. For example, Cromer teaches several examples wherein tampering of a computer require irrevocable conditions to prevent theft of the contents of the computer. See Cromer, col. 2, lines 1-57, and Figure 5. It would be obvious to one of ordinary skill in the art at the time the invention was made for the two conditions to be irrevocable to ensure the privacy of data within a device. See Cromer, col. 1, line 33-col. 2, line 64. The aforementioned covers claim 25.

32. As per claims 26 and 27, Maillard covers an apparatus as outlined above in the claim 25 rejection under 35 U.S.C. 103(a). In addition, at least one key portion is stored in ROM as outlined above. Further, the limitation as specified in claim 26 is a design choice implementation of the limitations defined in claim 25. See applicant's specification, page 14, lines 6 and 7. It would be obvious to one of ordinary skill in the art at the time the invention was made for the first irrevocable condition comprises programming ON a first certain bit of the one-time programmable ROM, and wherein the second irrevocable condition comprises programming ON a second certain bit of the one-time programmable ROM. Motivation for such an implementation enables a simple means of accessing key data contingent on a first and second irrevocable condition as known to one of ordinary skill in the art of circuit design. The aforementioned cover claims 26 and 27.

33. As per claims 10-12, they are method claims corresponding to claims 2 and 25-27, and they do not teach or define above the information claimed in claims 2 and 25-27. Therefore, claims 10-12 are rejected as being obvious over Maillard in view of Fielder, Reardon, Habersetzer and Cromer for the same reasons set forth in the rejections of claims 2 and 25-27.

34. As per claims 22-24, they are apparatus claims corresponding to claims 14 and 25-27, and they do not teach or define above the information claimed in claims 14 and 25-27. Therefore, claims 22-24 are rejected as being obvious over Maillard in view of Fielder, Reardon, Habersetzer and Cromer for the same reasons set forth in the rejections of claims 14 and 25-27.

35. As per claims 28-30, they are method claims corresponding to claims 25-27, and they do not teach or define above the information claimed in claims 25-27. Therefore, claims 28-30 are rejected as being obvious over Maillard in view of Fielder, Reardon, Habersetzer and Cromer for the same reasons set forth in the rejections of claims 25-27.

Allowable Subject Matter

36. Claims 9 and 21 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, second paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Ryan U.S. Patent No. 5,513,260.

Blatter et al. U.S. Patent No. 5,754,651.

Blatter et al. U.S. Patent No. 6,016,348.

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
July 28, 2004

Gilberto

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100